CIO Security Committee Meeting
Minutes
September 13, 2006

Present: Lesa Quinn, R.J. Hellstern, Todd Waddell, John Wolf, Mark Wise, Lyle Hervey, Brent McManus, Marianne Mickelson, Greg Fay, Calvin Moore, Deb Castillo, Verne Logan, Liz Murray, Shane Ludwig, Amanda Swangel, Brad Huyser, Diana Thompson

Lesa Quinn opened the meeting. Lesa reported that we would be hearing and seeing a demonstration from WinMagic Corporation regarding their Secure Doc Encryption software for laptops. This software could be used to comply with the new Laptop Encryption Standard that is now in the "review stage". The committee discussed the software and licensing issues after the demonstration. Cost - $975 for server software and $100 per device. You will want to alert your managers of this anticipated expense.

Contact:
Jim Armstrong
National Account Manager
WinMagic Disk Encryption
Work: 901-502-7000 Ext. 222
Mobile: 416-930-6910
Email: jim.armstrong@winmagic.com
Web site to visit: www.winmagic.com

1. There will be a cyber security exercise next year. Projected date is June 2007. Lesa Quinn is looking for several volunteers to help with the exercise.
2. State Security Officer is still working through the standards we have discussed the past few months. He is on the agenda for the TGB. Not guaranteed to get approval from TGB this month as they have an extremely full agenda.
3. State Security Officer discussed three standards that he is working to get addressed by the TGB. All agencies will be required to comply with these standards
    a. Laptop encryption
        i. Pre-boot encryption for all laptops
        ii. May be able to exclude some laptops if agency director signs a statement stating no confidential data exists on the laptop.
        iii. Laptop encryption still needs to address issues such as VPN access
        iv. CIO Security council viewed a demonstration for WinZip encryption products. This is the company which provides Windows encryption services for the NSA (National Security Agency)
    b. Also looking at a standard for removable media. There is a driving need for this as removable media is now able to hold large amounts of data which can leave agencies vulnerable to staff using unauthorized devices to store sensitive and/or confidential data. ISO will work with CIO security council to define removable media encryption standards
    c. Data Classification
        i. Working to identify standards for classifying data as sensitive, confidential, etc.
        ii. ISO will work to define standards but it will be up to agencies to classify their own data

d. Target dates
    i. Recognizing changes takes time and money, some of the target dates have been slated for the next fiscal year to give agencies the ability to draw from two fiscal years for necessary resources
    ii. March 1, 2007 is target date for the data classification
    iii. August 31, 2007 is the target date for the laptop encryption
    iv. March 1, 2007 is the target date for the encryption of removable media
e. Cyber Response Team
    i. There was discussion a year ago about a Security Incident Response Team. Identified a greater need for this after last week's incident with a worm infiltrating some state information systems. Idea is for there to be a central place where information is gathered, analyzed and shared.
    ii. Proposal is to have a core group that is the manager of an incident. These will be the individuals who are passing along information to all state agencies and will be looking at the big picture of any particular incident. This will be a seven member team, which will include the following representatives: CISO – 1; ITE – 1; ICN – 1; HLS – 1. And three individuals from other agencies. There will also be two alternates. Once the Cyper Response Team is activated all agencies will report network incidents to the team
    iii. Incidents and responses to incidents will be ranked as: Low, Medium, High
    iv. CISO is working to get the Iowa Interactive web site up and running.
f. Marketing
    i. Discussed how IT can get more information out to users in all agencies.
    ii. Spot Checks. Recommended that all agencies do spot checks as another way to check for users who are leaving passwords under keyboards or on monitors; who is walking away from their desk and leaving their desktop unattended and vulnerable to the public, etc
    iii. Options for training
        1. There is a free 2-hour DVD available to agencies. This is a videotape of training received approximately a year ago from a security professional. Has very good content
        2. Also some online training available by contacting CISO but some agencies felt that this training was not as good as the DVD
        3. HLS – has given states a kit for training which provides general security awareness. This has not been passed around much between agencies
        4. CISO would stress spot checks and educating managers as first-line protection for security integrity

Templates distributed: Employee Separation Checklist
Service Request Form
Network Administrator and System Administrator Separation Checklist

Next meeting will be: Wednesday, October 11, 2006 at 1:30 p.m.
Justice Bldg, Rm 165
Any suggested topics – please email Lesa Quinn at Lesa.Quinn@iowa.gov